Bezpečnost internetového bankovnictví (2)

V návaznosti na článek v minulém čísle ST se budeme věnovat tomu, jaká je skutečná (nikoli vysněná) realita fungování principů infrastruktury veřejných klíčů (PKI) a jak se toto spolu s jinými aspekty může promítat do bezpečnosti internetového bankovnictví.

Internet neposkytuje žádnou bezpečnost

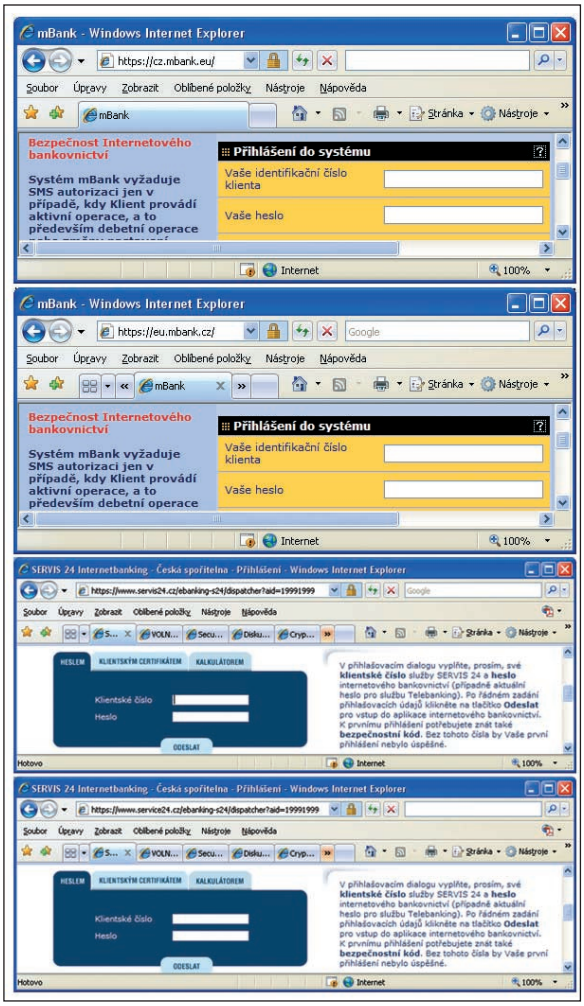
Na tom, že internet sám o sobě neposkytoval a neposkytuje žádnou bezpečnost, se s předními řečníky mezinárodních bezpečnostních konferencí snadno shodneme. Co je základním zdrojem potíží? Je to enormní technická a organizační složitost této sítě a jejích dílčích podsítí, kde bezpečnost je především organizační a poté teprve technická záležitost. Pravděpodobnost úspěšného odražení všech útoků na technické i organizační úrovni tak na cestě od klientova počítače do jeho banky exponenciálně klesá. Pokud je cesta krátká, nemusí se jednat o katastrofu. Je-li delší a navíc dynamická, je napadení spojení (únos spojení, útok na DNS atd.) jen otázkou momentální nálady útočníka. Kryptografie, konkrétně PKI, měla zjednat nápravu.

Cíl PKI

Cílem PKI bylo uživateli internetového bankovnictví poskytnout nějaký opěrný bod v moři té nejistoty. Konkrétně to měl být a stále je certifikát nějakého veřejného klíče – například serveru banky. Ten mu za prvé potvrdí, že komunikuje s bankou (identifikace a autentizace), a za druhé pomocí veřejného klíče z tohoto certifikátu zajistí šifrování komunikace s bankou (soukromí). Jenže v tomhle systému bohužel málokdo za něco zodpovídá. Zvykli jsme si, že výrobce SW nezodpovídá za to, co jeho SW dělá, a že s tím musíme souhlasit při potvrzování licence. Totéž zjistíme u celé slavné PKI na internetu. Jde jenom o to, abychom se oprostili od reklamních pohádek a přestali se tomu konečně divit.

HTTPS, SSL, TLS

Základem komunikace s bankou je protokol HTTP a jeho šifrovaná verze HTTPS. K šifrování se používají návazné protokoly SSL/TLS, proto certifikáty pro bankovní servery bývají nazývány SSL-certifikáty. Při navazování spojení si klientův PC obvykle stáhne bankovní certifikát, vygeneruje náhodná data, zašifruje je pomocí veřejného klíče z certifikátu serveru a odešle. Server je svým privátním klíčem dešifruje a následně použije pro šifrování spojení. Vlastní spojení se navazuje na základě informací z certifikátu, který obsahuje polidštěnou adresu serveru banky (zcela výjimečně i IP adresu).



Obr. 1 Pravý a falešný web, račte si vybrat a přihlásit se

Prohlížeč klienta má seznam důvěryhodných certifikačních autorit (CA) a při navazování šifrovaného spojení postupuje přibližně takto:

- Je certifikát, který jsem obdržel, podepsaný CA z mého seznamu?
- Je adresa, na kterou se připojuji, adresou zmíněnou v certifikátu?
- Pokud ne, zobraz varování

Ověření protistrany

A teď přejdeme do reality a zkusíme se vžít do role klienta, který zadá třeba www.mbank.cz a pak klikne na „přihlásit se“ k internetovému bankovnictví. Je přesměrován na https://cz.mbank.eu/ a objeví se mu jeho známá úvodní obrazovka. Ti obezřetnější klienti zkontrolují zámeček vedle adresy a pak už zadávají ID a heslo. Na základě obehrané písničky „zámeček vše vyřeší“ (viz minulé číslo ST) si jsou jisti, že komunikují s bankou (*obr. 1*).

Necháváme se (s)vést

Jsme přesvědčeni, že většina klientů, kdyby byla přesměrována na jakoukoliv z adres https://eu.mbank.cz/ nebo https://cz.mbanka.eu/ nebo https://mbanka.eu.cz/ nebo na tisíc jiných variant a vedle adresy se objevil zámeček, ničeho si nevšimne. Bohužel není problém zcela legálně na takový web zakoupit SSL certifikát, dokonce nejnovější „superbezpečný“ tzv. EV certifikát (extended validation), o němž budeme ještě hovořit dále. Říkáme bohužel, ale kdyby to bylo zakázáno, tak by si ani mbanka ani nikdo jiný nemohl legálně zakoupit certifikát. Z hlediska certifikačních politik a jiných pravidel nikdo neudělá žádnou chybu. Navíc některé uvedené domény jsou nejen volné, ale i legálně fungující domény zavedených firem. Pokud je útočník chytrý, provede miniaturní změnu adresy, které si může všimnout opravdu jen málokdo. A to je jen jeden z mnoha technických problémů na cestě mezi klientem a bankou. Třeba u ČS je uživatel přesměrován z https://www.servis24.cz na složitou adresu https://www.servis24.cz/ebanking-s24/dispatcher?aid=19991999, kterou banka důsledně uvádí i v návodech. Nikdo tak dlouhou adresu nezadává a nechává se na ni navést z hlavní stránky banky a pod., což platí obecně u mnoha bank. Zvyk „nechat se navést“, může drzý útočník snadno zneužít a klienta navést k sobě. S těmito zvyklostmi a do takto neurčitého prostředí skoro všichni klienti zadávají ID a heslo. Namátkou jsme vyzkoušeli http://www.service24.cz/. Je to web asistenční a odtahové firmy, která existuje od roku 1994. Tato firma má jistě právo si u Verisign zakoupit kvalitní EV certifikát třídy 3 (stejně jako ČS a. s.) pro své potřeby třeba interní sítě. Útočníkovi by se pak stačilo nabourat do jejich webu a umístit tam stránku https://www.service24.cz/ebankings24/dispatcher?aid=19991999, aniž by o tom odtahová firma a ČS a. s. měla tušení. Zbývá jen technická hračka, tedy na vhodném DNS serveru nebo LAN síti přesměrovat vybranou část požadavků (když útočník nebude hamoun) elektronického bankovnictví z adresy www.servis24.cz na www.service24.cz. Klienti neuvidí nic jiného než obvykle (*obr. 1*). Pokud si tedy nevšimnou změny servis24 na service24 v oné dlouhé adrese. Pokud ne, jsou již

plně v rukou útočníka. Útočník může takto třeba rok pasivně získávat hesla nebo provádět aktivní útok MITM, jak jsme o něm psali v minulém čísle ST. Klienti téměř všech bank na světě jsou na tom stejně, když přistupují na internet. Všichni toto a jiná podobná rizika podstupují, banky na 100 % vědomě, klienti na 99,99 % nevědomě.

Paranoici

„Paranoidní“ klienti mohou přehlédnout změnu v adrese, ale mohou se chtít ještě před zadáním hesla přesvědčit o pravosti webu, na který se dostali. Kliknou tedy na ikonu zámečku (*obr. 2*).

Extra paranoici

Ale pokračujme dále. Klient trvá na ověření a ve výše uvedeném informačním okně si nechá „zobrazit certifikáty“.

Teď už je jedno, jestli hovoříme o platném certifikátu útočníka nebo platném certifikátu banky, a je jedno, kde se klient nachází, zda na webu útočníka nebo banky. Ve všech případech klient vidí, že certifikát verifikovala jiná CA než očekával. Nějaká „www.verisign.com/CPS Incorp.by Ref. LIABILITY LTD.(c)97 VeriSign.“ Zná ji? Četl její certifikační politiku? Nebo se ho zeptejme, jestli ví, kde ji najít? Nebo jinak, byl by spokojen s tím, že by certifikát pro bankovní server vystavila CA www.verisign.com/CPS Incorp. by Ref. LIABILITY LTD.(c)97 VeriSign? Všimne si, že se ta jména liší mezerou uprostřed nebo tečkou na konci jména? Ví náš klient o tom, že na internetu je cca 800 000 dalších „zámečkových“ stránek?

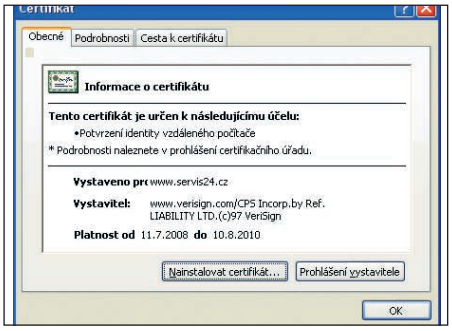
Ultra paranoici

Kdyby náš klient byl ultra paranoidní a chtěl si opovážlivě ověřit i vystavitele certifikátu (stačí kliknout na tlačítko „Prohlášení vystavitele“), dostal by se na stránku http://www.verisign.ch/repository/rpa.html. Není tam prohlášení vystavitele, ale právní dokument, dohoda, mající pět stran. Říká se v ní, že pokud klient něco od Verisignu chce, musí s ní souhlasit. Dále je zřejmé, že „nejlepší“ jsou certifikáty třídy 3 a že náhrada případné škody je omezena. Dále si klient podle dohody musí přečíst certifikační politiku (CP) na adrese www.verisign.com/repository/cps. Dle definice jejích tvůrců „je to dokument, který je čas od času měněn a reprezentuje způsob práce... [Verisignu]“. Když klient bude mít štěstí, zjistí na některé ze 121 stran, že Verisign nijak nezodpovídá za „Non-verified Subscriber Information“, což podle slovníku znamená „jakoukoliv informaci, kterou žadatel o certifikát poskytl a včlenil do certifikátu, která nebyla potvrzena... [Verisignem]“. Která to je, musí klient opět vyhledat v certifikační politice.

Super paranoici

Pokud klient ještě vydržel, jde zkoumat CP, a to rovnou pro ty nejlepší dnešní certifikáty – třída 3, a s tzv. rozšířenou kontrolou (extended validation, EV). Na straně 65 v CP je uvedeno, že odpovědnost za EV certifikáty řeší dodatek B1. Co tam klient nalezne, uvádíme již bez komentáře: In cases where VeriSign has issued and managed the EV Certificate in compliance with the Guidelines and its CPS, VeriSign shall not be liable to the EV Certificate Subscribers or Relying Parties or any other third parties for any losses suffered as a result of use or reliance on such EV Certificate.

Obr .2 Identifikace



Obr. 3 Vystavitel certifikátu

Mega paranoici

Jenže náš neodbytný a bezpečnosti lačný klient jistě dojde k jednoduššímu řešení. Zavolá na help-line banky. Tam mu po hodině přepojování a vysvětlování přečtou sériové číslo certifikátu, jeho miniaturu a další údaje. Klient je ověří a je spokojen. Z předchozího víme, že někteří klienti se v tuto dobu už mohou nacházet na webu útočníka, který jim na jejich přání zobrazí jakýkoliv jiný certifikát, příjemnější (i když vymyšlenou) certifikační politiku s vysokými zárukami a pojistným, číslo na help-line, které je stále obsazeno, a poukaz na buřty s mákem jako bonus za projevenou důvěru.

Jde to i jinak?

PKI je nástroj, který může být bezpečný, pokud jsou dosti tvrdě splněny určité předpoklady. Aby se k nim přiblížily, některé banky z opatrnosti zavedly certifikáty klientů (na čipových kartách, apod.). Tím se dokonce může ustavit oboustranně důvěryhodný a šifrovaný tunel v rámci internetového spojení. Jenže práce s certifikátem (na čipové kartě nebo bez ní) není tak příjemná jako zadání hesla do prohlížeče. Je to i drahé. A nakonec, jde nejen o certifikát, ale i o celkovou bezpečnost, a tu banka nemůže klientovi zajistit ani zlatým certifikátem. Možná to tak vypadalo, ale na banku se zlobit nemůžeme. Aby PKI fungovala, musela by klienta vybavit také svým počítačem s ověřeným operačním systémem, aplikacemi a další ochranou, včetně ochrany certifikátů. Pak by princip PKI začal fungovat. A byla to právě obecná rizika počítačové bezpečnosti, uživatelská neprůhlednost a omezený přínos PKI, které vedly k tomu, že tato cesta je opouštěna. To není chyba matematických vzorců a konečně ani bankovních architektů, to je důsledek otevřenosti internetu. Věříme, že PKI se vrátí, ale v jiné technické podobě, bezpečnosti a uživatelské přítulnosti. Jak to můžeme tak vědět?

Jde to i jinak

...a také to i jinak vypadá, chtělo by se hned dodat. Vezměme příklady, kdy PKI funguje. Jsou to obvykle malé, střední i mezinárodní vnitropodnikové informační systémy, které jsou založené na interní CA, na centrální správě počítačů a tvrdě vynucených bezpečnostních politikách. Všechna tato prostředí mají jednu zásadní věc společnou, a to je velmi nízká variabilita na straně koncového uživatele. Jen díky tomu může být uživatel uchráněn. Uchráněn před sebou samým, aby se nenachytal na úlisný pokus útočníka. PKI je nástroj, o který bezpečnostní architekti určitě nebudou chtít přijít. Zároveň už ale (snad) ví, že ho nemohou dát přímo do rukou uživatele. Musí ho nějak zabalit, zakomponovat a zatajit kamsi do jednoúčelových předmětů sloužících například právě ke komunikaci s bankou. Jak přesně to bude vypadat si zatím odhadnout netroufáme, ale pár příkladů za všechny – napadlo by vás, když u pokladny platíte víkendový nákup svou elektronickou platební kartou, že jste právě nejméně jednou skrytě využili služeb úzce specializovaného PKI a několika certifikačních autorit? Vidíte nějaké certifikáty a zámečky, když používáte svůj elektronický pas na letišti? Tak takhle nějak to asi bude vypadat…

Závěr

Chtěli jsme ukázat, že co ve vnitropodnikovém pojetí může být naprosto úžasné a neprůstřelné, se po natažení na rozměry internetu může proměnit v analogii minového pole. A certifikát? V kryptografii je to velmi krásný a průzračný diamant. Pokud ho vložíme do bezpečného prostředí, bude nás oslňovat svojí nádherou a dokonalostí.

Poznamenejme, že uváděné příklady se vztahují k účtům 1. z autorů.

Vlastimil Klíma, Tomáš Rosa,
v.klima@volny.cz, tomas.rosa@rb.cz

LITERATURA

[1] E-archivy http://cryptography.hyperlink.cz, http://crypto.hyperlink.cz